FRANKLIN D. AZAR & ASSOCIATES
Ivy Ngo, California SBN 249860
ngoi@fdazar.com
14426 East Evans Ave
Aurora, CO 80014
Telephone: 303-757-3300
Facsimile: 720-213-5131

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

REBECCA A. KING, AN INDIVIDUAL AND CALIFORNIA RESIDENT, DOMINIQUE MARTIN, AN INDIVIDUAL AND NEW JERSEY RESIDENT, RUBIN K. JOHNSON, AN INDIVIDUAL AND COLORADO RESIDENT, AND ROBERT E. NEWBORN, AN INDIVIDUAL AND COLORADO RESIDENT,

Plaintiffs,

vs

FACEBOOK, INC.,

Defendant

Case No.: Number

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

(1) UCL – Unlawful Business Practice
(2) UCL – Unfair Business Practice
(3) UCL – Fraudulent/Deceptive Business Practice
(4) Deceit by Concealment
(5) Negligence
(6) Breach of Implied Contract
(7) Violation of Colorado Consumer Protection Act
(8) Violation of Colorado Security Breach Notification Act
(9) Violation of California Customer Records Act
(10) Violation of New Jersey Customer Security Breach Disclosure Act
(11) Violation of New Jersey Consumer Fraud Act

TABLE OF CONTENTS

For their Class Action Complaint, Plaintiffs Rebecca A. King, Dominique Martin, Rubin K. Johnson, and Robert E. Newborn, ("Plaintiffs"), on behalf of themselves and all others similarly situated, allege the following against Defendant Facebook, Inc. ("Defendant" or "Facebook"), based on personal knowledge as to Plaintiffs, and Plaintiffs' own acts and on information and belief as to all other matters based upon, *inter alia*, the investigation conducted by and through Plaintiffs' undersigned counsel:

SUMMARY OF CASE

1. This case involves a data breach Facebook announced on September 28, 2018, wherein the PII of 50 million of its Users was exposed due to a flaw in Facebook's code that allowed hackers and other nefarious users to take over User accounts and siphon off personal information for unsavory and illegal purposes ("September 2018 Data Breach").

2. Facebook operates a social networking website that allows people to communicate with their family, friends, coworkers, and acquaintances. Facebook also develops technologies that facilitate the sharing of information, photographs, website links, and videos. Facebook purports to allow its users ("Facebook Users" or "Users") the ability to share and restrict information based on their own specific criteria. By the end of 2017, Facebook had more than 2.2 billion active Users.

3. As part of the sign-up process and as a consequence of interacting with their social network, Facebook Users create, maintain, and update profiles containing significant amounts of personal information, including their names, birthdates, hometowns, addresses, locations, interests, relationships, email addresses, photos, and videos, amongst others, referred to herein as "PII."

4. In an ongoing investigation, Facebook recently revealed that its Users' personal information was subject to a massive data security breach in September 2018, affecting approximately 50 million Facebook Users' PII. Facebook publicly exposed details of the September 2018 Data Breach for the first time in a statement on September 28, 2018. According to the statement and subsequent press call, Defendant learned of the breach as early as September

16, 2018,[1] but has not yet directly informed or notified Facebook Users that their PII may be compromised as a result of the breach. Rather, Facebook states that it began "logging users out" on the evening of September 27, 2018, but did not provide Users with any reason for being logged out. The statement further admitted that "attackers exploited a vulnerability in Facebook's code that impacted "View As" a feature that lets people see what their own profile looks like to someone else. This allowed them to steal Facebook access tokens which they could then use to take over people's accounts. Access tokens are the equivalent of digital keys that keep people logged in to Facebook so they don't need to re-enter their password every time they use the app."[2] The vulnerability in Facebook's code was introduced in July 2017, and Facebook is currently unaware of how long hackers have had access since that time.[3]

5. As a result of Defendant's failure to maintain adequate security measures and timely security breach notifications, Facebook Users' personal and private information has been compromised and remains vulnerable. In fact, according to Facebook, they "have yet to determine whether those accounts were misused or any information accessed."[4] Further, Facebook Users have suffered an ascertainable loss in that they must undertake additional security measures, some at their own expense, to minimize the risk of future data breaches including, without limitation, canceling credit cards associated with their Facebook accounts and changing passwords to Facebook, Instagram, and other linked accounts. However, due to Facebook's ongoing and incomplete investigation, Facebook Users have no guarantee that the above security measures will in fact adequately protect their personal information. As such, Plaintiffs and other Class Members have an ongoing interest in ensuring that their personal information is protected from past and future cybersecurity threats.

6. This Class Action Complaint is filed on behalf of all persons in the United States described more fully in the following sections, whose PII was compromised in the

[1] "Afternoon Press Call," Facebook Newsroom, Sept 28, 2018, transcript available at https://fbnewsroomus.files.wordpress.com/2018/09/9-28-afternoon-press-call.pdf (last visited Oct 1, 2018).

[2] "Security Update," Facebook Newsroom, available athttps://newsroom.fb.com/news/2018/09/security-update/ (last visited Oct. 1, 2018)

[3] *See* https://techcrunch.com/2018/09/28/everything-you-need-to-know-aboutfacebooks-data-breach-affecting-50m-users/ (last visited Oct. 1, 2018)

[4] *Id.*

September 2018 Data Breach.

JURISDICTION AND VENUE

7. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least one class member is a citizen of a state different from Defendant and is a citizen of a foreign state. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

8. Venue is proper under 28 U.S.C. § 1391(c) because Defendant is a corporation that does business in and is subject to personal jurisdiction in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claims in this action occurred in or emanated from this District, including the decisions made by Facebook's governance and management personnel that led to the breach. Further, Facebook's terms of service governing users in the United States provides for California venue for all claims arising out of Plaintiffs' relationship with Facebook.

PARTIES

A. Plaintiffs

9. Plaintiff Rebecca A. King ("King") is a resident and citizen of California. Plaintiff King opened a Facebook account and used it for at least nine years, entrusting Facebook with and aggregating PII for this time period. On or about September 28, 2018, Plaintiff King received a notice from Facebook informing her that her account and PII may have been compromised in the September 2018 Data Breach. In addition to the damages detailed herein, the September 2018 Data Breach has caused Plaintiff King to be at substantial risk for further identity theft.

10. Plaintiff Dominique Martin ("Martin") is a resident and citizen of New Jersey. Plaintiff Martin opened a Facebook account and used it for at least ten years, entrusting Facebook with and aggregating PII for this time period. On or about September 28, 2018, Plaintiff Newborn received a notice from Facebook informing her that her account and PII may have been compromised in the September 2018 Data Breach. In addition to the damages detailed

herein, the September 2018 Data Breach has caused Plaintiff Martin to be at substantial risk for further identity theft.

11. Plaintiff Rubin K. Johnson ("Johnson") is a resident and citizen of Colorado. Plaintiff Johnson opened a Facebook account and used it for at least seven years, entrusting Facebook with and aggregating PII for this time period. On or about September 28, 2018, Plaintiff Johnson received a notice from Facebook informing him that his account and PII may have been compromised in the September 2018 Data Breach. In addition to the damages detailed herein, the September 2018 Data Breach has caused Plaintiff Johnson to be at substantial risk for further identity theft.

12. Plaintiff Robert E. Newborn ("Newborn") is a resident and citizen of Colorado. Plaintiff Newborn opened a Facebook account and used it for at least seven years, entrusting Facebook with and aggregating PII for this time period. On or about September 28, 2018, Plaintiff Newborn received a notice from Facebook informing him that his account and PII may have been compromised in the September 2018 Data Breach. In addition to the damages detailed herein, the September 2018 Data Breach has caused Plaintiff Newborn to be at substantial risk for further identity theft.

B. Defendant

13. Defendant Facebook, Inc. is a Delaware corporation with its principal executive offices located at 1601 Willow Road, Menlo Park, California 94025. Facebook's securities trade on the NASDAQ under the ticker symbol "FB."

14. At all relevant times, Defendant was and is engaged in the business of operating a social networking website and mobile application in San Mateo County and throughout the United States of America.

FACTUAL BACKGROUND

A. Facebook Collects and Stores PII for its Own Financial Gain

15. Most of Facebook's revenue comes from the sale of targeted advertising services. For example, during 2017, Facebook generated $40.65 billion in revenue, of which $39.94 billion

was advertising revenue.[5]

16. Facebook offers advertising services to its customers (advertisers) that include or have included at various points in time, among other things, assisting customers in developing and creating advertisements and advertising strategies, obtaining information about Facebook Users from Facebook's website and third-party sources, compiling user data and maintaining databases of information about Facebook Users, developing a marketing and advertising strategy to target and exclude certain groups of Facebook Users from receiving advertisements, tracking and evaluating the effectiveness of advertisements and Facebook User targeting strategies, implementing advertising campaigns, and delivering advertisements to Facebook Users, including via News Feed.

17. Facebook's customers can use Facebook's advertising services to target its Users with specific attributes. Facebook applies its own algorithm to categorize Users and to determine which Users and groups of Users will be targeted to receive advertisements via its advertising platform. As stated on Facebook's website: "With our powerful audience selection tools, you can target people who are right for your business. Using what you know about your customers—like demographics, interests and behaviors—you can connect with people similar to them."

18. Facebook also provides detailed analytical data to advertisers on how their ad campaigns are performing, including among certain groups of Facebook Users with specified attributes and characteristics that the advertiser seeks to target. By monitoring this data and providing this information to its customers on an ongoing basis, Facebook captures consumer behavior, profile, preferences, lifestyle, and other attributes which allow Facebook to run targeted ads. This enables advertisers to specify the groups of users that will be targeted to receive the advertisements.

19. Targeting advertising of this nature requires Facebook to compile an enormous amount of Personal Information from its users, including PII. This data Facebook has about its

[5] Facebook, Form 10-K, for the fiscal year ended December 31, 2017, at 34.

Users is highly valuable. The average cost per click for an online Facebook ad was $1.72 in 2017,[6] and the average U.S. Facebook User is reportedly worth about $200 a year.[7]

20. Despite the fact that substantially all of Facebook's revenue comes directly from its collection of PII, on information and belief, Defendant failed, and continues to fail, to provide adequate protection of its Users' personal and confidential information and has egregiously failed to provide sufficient and timely notice or warning of potential and actual cybersecurity breaches to its Users.

21. At all relevant times, Facebook has made several assurances to its Users that their privacy and security is of utmost importance to Facebook, and its Users have relied on those assurances in providing Facebook with their PII. In fact, Facebook's Data Policy represents to its Users that Facebook "Promote[s] safety, integrity, and security" by "us[ing] the information we have to verify accounts and activity, combat harmful conduct, detect and prevent spam and other bad experiences, maintain the integrity of our Products, and promote safety and security on and off of Facebook Products."[8] Facebook has failed to provide the security consistently promised to its Users prior to the September 2018 Data Breach, including that it was "putting stronger protections in place to prevent future abuse of our platform."[9]

22. Despite these assurances, Facebook publicly revealed on September 28, 2018 that its Users' personal information was subject to a massive data security breach. According to Facebook's statement publicly exposing details of the September 2018 Data Breach for the first time and subsequent press call, Defendant learned of the breach as early as September 16, 2018,[10] but has not yet directly informed or notified Facebook Users that their PII may be compromised as a result of the breach. Rather, Facebook stated that it began "logging users

[6] Mark Irvine, Facebook Ad Benchmarks for YOUR Industry [New Data] *available at* https://www.wordstream.com/blog/ws/2017/02/28/facebook-advertising-benchmarks (last visited Oct. 10, 2018).

7 Sam Harnett, Here's How Much You Are Worth To Facebook In Dollars and Cents, *available at* https://www.kqed.org/news/11661387/heres-how-much-you-are-worth-to-facebook-in-dollars-andcents (last visited Oct. 10, 2018).

[8] Facebook, Data Policy, https://www.facebook.com/privacy/explanation (last visited Oct. 1, 2018).

[9] Facebook Help, How is Facebook working to keep its community safe?, available at https://www.facebook.com/help/208040513126776?helpref=popular_topics (last visited Oct. 1, 2018).

[10] https://fbnewsroomus.files.wordpress.com/2018/09/9-28-afternoon-press-call.pdf (last visited Oct. 1, 2018)

out" the evening of September 27, 2018, without providing Users with any reason for being logged out. The statement further admitted that "attackers exploited a vulnerability in Facebook's code that impacted "View As" a feature that lets people see what their own profile looks like to someone else. This allowed them to steal Facebook access tokens which they could then use to take over people's accounts. Access tokens are the equivalent of digital keys that keep people logged in to Facebook so they don't need to reenter their password every time they use the app.[11] The vulnerability in Facebook's code was introduced in July 2017, and Facebook is currently unaware of how long hackers have had access since that time.[12]

23. As a result of Defendant's failure to maintain adequate security measures and timely security breach notifications, Facebook Users' personal and private information has been compromised and remains vulnerable. In fact, according to Facebook, it has "yet to determine whether those accounts were misused or any information accessed."[13] Further, Facebook Users have suffered an ascertainable loss in that they must undertake additional security measures, some at their own expense, to minimize the risk of future data breaches including, without limitation, canceling credit cards associated with their Facebook accounts and changing passwords to Facebook, Instagram, and other linked accounts. However, due to Facebook's ongoing and incomplete investigation, Facebook Users have no guarantee that such security measures will in fact adequately protect their personal information. Accordingly, Plaintiffs and other Class Members have an ongoing interest in ensuring that their personal information is protected from past and future cybersecurity threats.

24. The insufficient security policies and procedures implemented by Defendant is a material fact that a reasonable consumer would consider when deciding whether to create a Facebook account and provide Defendant with personal and confidential information. Had Plaintiffs and other Class Members known that Defendant failed to employ necessary and

[11] "Security Update," Facebook Newsroom, available at https://newsroom.fb.com/news/2018/09/security-update/ (last visited Oct. 1, 2018).

[12] See https://techcrunch.com/2018/09/28/everything-you-need-to-know-about¬facebooks-data-breach-affecting-50m-users/ (last visited Oct. 1, 2018).

[13] *Id.*

adequate protection of their personal information, they would not have created a Facebook account, or they would have limited the PII they shared with Facebook. Plaintiffs and other Class Members should have been able to rely upon Facebook's "Privacy Principles" ensuring that "We work around the clock to help protect people's accounts, and we build security into every Facebook product. Our security systems run millions of times per second to help catch threats automatically and remove them before they ever reach you."[14]

25. This case involves the continuing and absolute disregard with which Defendant has chosen to treat the PII of account holders who utilize Facebook's social media platform. While this information was supposed to be protected, Facebook – without authorization – exposed that information to third parties through lax and non-existent data safety and security policies and protocols.

26. Facebook's Terms of Service state that the Facebook user is the owner of all of his or her data. Facebook's representation to Plaintiffs and Class Members that "Protecting people's information is at the heart of everything we do" was, in fact, a misrepresentation[15] and one which Plaintiffs and Class Members relied upon.

27. In addition, Facebook made the following representations to its Users:

- "you have control over who sees what you share on Facebook."[16]
- "We have top-rate security measures in place to help protect you and your data when you use Facebook."[17]
- "Your activity (ex: posting a status or sending a message) is encrypted, which means it's turned into code so people can't access it without your permission."[18]
- "When it comes to your personal information, we don't share it without your

[14] https://www.facebook.com/about/bascis/privacy-principles

[15] Matthew Rosenberg, Nicholas Confessore, and Carole Cadwalladr, How Trump Consultants Exploited the Facebook Data of Millions, THE NEW YORK TIMES (March 17, 2018) https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html (last visited August 30, 2018).

[16] Facebook, *Privacy Basics*, https://www.facebook.com/about/basics (last visited August 30, 2018)

[17] Facebook, How You're Protected, https://www.facebook.com/about/basics/stay-safe-and-secure/how-youre-protected (last visited August 30, 2018).

[18] *Id.*

permission (unless required by law)."[19]

- "Facebook gives people control over what they share, who they share it with, the content they see and experience, and who can contact them."[20]

28. At all relevant times, Facebook has maintained a Data Use Policy on its website which advised Facebook users, in part:

> Granting us permission to use your information not only allows us to provide Facebook as it exists today, but it also allows us to provide you with innovative features and services we develop in the future that use the information we receive about you in new ways. While you are allowing us to use the information we receive about you, you always own all of your information. ***Your trust is important to us, which is why we don't share information we receive about you with others unless we have:***
>
> - ***received your permission***
> - ***given you notice***, such as by telling you about it in this policy; or
> - removed your name and any other personally identifying information from it.

(Emphases Added).[21]

29. Even before Facebook's Chief Executive Mark Zuckerberg made statements (and before Facebook provided a series of written responses) to Congress, he declared that "Every piece of content that you share on Facebook you own. . . . You have complete control over who sees it and how you share it".[22] Facebook users, including Plaintiffs and the Class Members, reasonably relied on Defendant's representations for the security of their PII in using Facebook and posting PII on Facebook.

30. On June 29, 2018, Facebook provided written responses to seven hundred questions the United States House of Representatives Commerce and Energy Committee had submitted to Facebook in April 2018. ("June 2018 Responses").[23]

31. In the June 2018 Responses, Facebook identified the types of data it collects

[19] *Id.*

[20] Facebook, Safety, https://www.facebook.com/safety (last visited August 30, 2018).

[21] Facebook, Data Use Policy, https://www.facebook.com/full_data_use_policy (last visited August 30, 2018)

[22] Gabriel Dance, Nicholas Confessore, and Michael LaForgia, *Facebook Gave Device Makers Deep Access to Data on Users and Friends*, THE NEW YORK TIMES (June 3, 2018) https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends¬data.html (last visited August 30, 2018)

[23] Facebook, Letter to House Commerce and Energy Committee, June 29, 2018, available at https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Wstate-ZuckerbergM-20180411-SD003.pdf (hereinafter, "Letter to House").

from users:

- Device attributes: information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.

- Device operations: information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).

- Identifiers: unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts people use, and Family Device IDs (or other identifiers unique to Facebook Company Products associated with the same device or account).

- Device signals: Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.

- Data from device settings: information users allow us to receive through device settings people turn on, such as access to their GPS location, camera, or photos.

- Network and connections: information such as the name of users' mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on users' network, so we can do things like help people stream a video.

- Cookie data: data from cookies stored on a user's device, including cookie IDs and settings.[24]

32. Despite Facebook's tumultuous 2018—including the Cambridge Analytica revelations, reading and collecting the contents of messages on Android Devices, and the device partnerships Facebook secretly entered into to share PII with other, unauthorized entities—Facebook's lax approach to data security resulted in the September 2018 Data Breach affecting 50 million users.

33. On March 19, 2018, *Bloomberg* published an article entitled "FTC Probing Facebook For Use of Personal Data, Source Says," disclosing that the U.S. Federal Trade

[24] Letter to House, at p. 112.

Commission ("FTC") was investigating whether Facebook violated the terms of a 2011 FTC consent decree regarding its handling of user data.[25]

34. Under the 2011 settlement with the FTC, Facebook "agreed to get user consent for certain changes to privacy settings" as part of a settlement of federal charges that it deceived Users and forced them to share more Personal Information than they had intended.[26]

B. PII is Very Valuable on the Black Market

35. The types of information compromised in the September 2018 Data Breach are highly valuable to identity thieves. The names, email addresses, recovery email accounts, telephone numbers, dates of birth, passwords, security question answers, and other valuable PII can all be used to gain access to a variety of existing accounts and websites.

36. Identity thieves can also use the PII to harm Plaintiffs and Class members through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[27]

[25] Bloomberg Markets, FTC Said to Probe Facebook on Personal Data Use, Bloomberg (March 19, 2018) https://www.bloomberg.com/news/videos/2018-03-20/facebook-said-to-face-ftc-probe-on-use-of-personal-data-video (last visited August 30, 2018)

[26] *Id.*

[27] The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan, Federal Trade Commission, 11 (April 2007), http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf.

37. To put it into context, as demonstrated in the chart below, the 2013 Norton report, based on one of the largest consumer cybercrime studies ever conducted, estimated that the global price tag of cybercrime was around $113 billion at that time, with the average cost per victim being $298 dollars. That number will no doubt increase exponentially after the PII of over 50 million users was leaked in the September 2018 Data Breach.

38. The problems associated with identity theft are exacerbated by the fact that many identity thieves will wait years before attempting to use the PII they have obtained. Indeed, in order to protect themselves, Class members will need to remain vigilant against unauthorized data use for years and decades to come.

39. Once stolen, PII can be used in a number of different ways. One of the most common is that it is offered for sale on the "dark web," a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and PII.[28] Websites appear and disappear quickly, making it a very dynamic environment.

40. Once someone buys PII, it is then used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

41. In addition to PII, a hacked Facebook account can be very valuable to cybercriminals. Since Facebook accounts are linked to a myriad of accounts, a hacked Facebook account could open up a number of other accounts to an attacker.

C. Facebook's Inadequate Data Security Allowed the Massive Breach of 50 Million User Accounts

42. On September 28, 2018, Facebook announced the "previously unreported attack

[28] Brian Hamrick, The dark web: A trip into the underbelly of the internet, WLWT News (Feb. 9, 2017 8:51 PM), http://www.wlwt.com/article/the-dark-web-a-trip-into-theunderbelly-of-the-internet/8698419.

on its network," exposing the PII of "nearly 50 million users."[29]

43. Facebook claimed it discovered the vulnerability "earlier this week," that it entirely fixed the vulnerability, and law enforcement was notified.[30]

44. However, Facebook did not know the origin or identity of the hackers. In fact, Facebook had not fully assessed the scope of the attack, despite its representations that the vulnerability was fixed.[31]

45. The vulnerability Facebook disclosed was a bug in its site's "view as" feature, which permits users to view their profiles posing as someone else, which, ironically, was built in to give users more control over their privacy.[32]

46. Guy Rosen, a vice president of product management at Facebook, admitted during the September 28, 2018 conference call that the September 2018 Data Breach was "complex" and "leveraged three separate bugs in Facebook's code that, once compounded, provided widespread access to user accounts."[33]

47. As Senator Mark Warner, a Democrat from Virginia, stated "This is another sobering indicator that Congress needs to step up and take action to protect the privacy and security of social media users," underscoring the lack of protections Facebook and other companies have when storing and securing the PII of millions of United States citizens.[34]

48. Unfortunately, despite numerous lapses in its approach to data security, Facebook still lacks the safeguards and protections for Users' PII, and that information remains at risk today and into the future, until Facebook is compelled to secure the PII stored on millions of United States citizens who are its Users.

CLASS ACTION ALLEGATIONS

49. Pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil

[29] Chris Mills, Facebook Says New Hack Leaded Data of 50 Million Users, BGR (Sept. 28, 2018) https://bgr.com/2018/09/28/facebook-data-breach-2018-yep-another-one

[30] Mike Issac and Sheera Frenkel, Facebook Network is Breached, Putting 50 Million Users' Data at Risk, NY Times (Sept. 28, 2018) https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *Id.*

Procedure, Plaintiffs, individually and on behalf of all others similarly situated, bring this lawsuit on behalf of themselves and as a class action on behalf of the following Class and Sub-Class:

> **Nationwide Class**: All persons who registered for Facebook accounts in the United States and whose PII was accessed, compromised, or stolen from Facebook in the September 2018 Data Breach.
>
> **Colorado Sub-Class**: All persons in Colorado who registered for Facebook accounts and whose PII was accessed, compromised, or stolen from Facebook in the September 2018 Data Breach.
>
> **California Sub-Class**: All persons in California who registered for Facebook accounts and whose PII was accessed, compromised, or stolen from Facebook in the September 2018 Data Breach.
>
> **New Jersey Sub-Class**: All persons in New Jersey who registered for Facebook accounts and whose PII was accessed, compromised, or stolen from Facebook in the September 2018 Data Breach.

50. Excluded from the Class are Defendant and any entities in which Defendant or its subsidiaries or affiliates have a controlling interest, and Defendant's officers, agents, and employees. Also excluded from the Class are the judge assigned to this action, members of the judge's staff, and any member of the judge's immediate family. Plaintiffs reserve the right to amend the Class and Sub-Class definition if discovery and further investigation reveal that the Class should be expanded or otherwise modified.

51. **Numerosity:** The members of each Class are so numerous that joinder of all members of any Class would be impracticable. Plaintiffs reasonably believe that Class members number hundreds of millions of people or more in the aggregate and well over 1,000 in the smallest of the classes. The names and addresses of Class members are identifiable through documents maintained by Defendant.

52. **Commonality and Predominance**: This action involves common questions of law or fact, which predominate over any questions affecting individual Class members, including:

a. Whether Defendant represented to the Class that it would safeguard Class members' PII;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant breached a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

d. Whether Class members' PII was accessed, compromised, or stolen in the September 2018 Data Breach;

e. Whether Defendant knew about the September 2018 Data Breach before it was announced to the public and failed to timely notify the public of the September 2018 Data Breach;

f. Whether Defendant's conduct violated Cal. Civ. Code § 1750, *et seq;*

g. Whether Defendant's conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, *et seq.;*

h. Whether Defendant's conduct violated the Consumer Records Act, Cal. Civ. Code § 1798.80 *et seq.;*

i. Whether Defendant's conduct violated the Online Privacy Protection Act, Cal. Bus. & Prof. Code § 22575, *et seq.;*

j. Whether Defendant's conduct violated § 5 of the FTC Act, 15 U.S.C. § 45, *et seq.;*

k. Whether Plaintiffs and the Class are entitled to equitable relief, including, but not limited to, injunctive relief and restitution; and

l. Whether Plaintiffs and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief.

53. As further indication of the common questions of law, Facebook's terms of service provides that "[f]or any claim, cause of action, or dispute you have against us that arise out of or relates to these Terms or the Facebook Products ("claim")…the laws of the State of California will govern these Terms of any claim."

54. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

55. **Typicality:** Plaintiffs' claims are typical of the claims of the other members of their respective classes because, among other things, Plaintiffs and the other Class members were injured through the substantially uniform misconduct by Defendant. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of other Class members arise from the same operative facts and are based on the same legal theories.

56. **Adequacy of Representation:** Plaintiffs are adequate representatives of the classes because their interests do not conflict with the interests of the other Class members they seek to represent; they have retained counsel competent and experienced in complex class action litigation and Plaintiffs will prosecute this action vigorously. The Class members' interests will be fairly and adequately protected by Plaintiffs and their counsel.

57. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other members of their respective classes are relatively small compared to the burden and expose the would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments, and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

58. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the members of the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of

Civil Procedure.

59. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Class members' PII was accessed, compromised, or stolen in the September 2018 Data Breach;

b. Whether (and when) Defendant knew about any security vulnerabilities that led to the September 2018 Data Breach before they were announced to the public and whether Defendant failed to timely notify the public of those vulnerabilities and the September 2018 Data Breach;

c. Whether Defendant's conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, *et seq.;*

d. Whether Defendant's representations that it would secure and protect the PII of Plaintiffs and members of the classes were facts that reasonable persons could be expected to rely upon when deciding whether to use Defendant's services;

e. Whether Defendant misrepresented the safety of its many systems and services, specifically the security thereof, and its ability to safely store Plaintiffs' and Class members' PII;

f. Whether Defendant concealed crucial information about its inadequate data security measures from Plaintiffs and the Class;

g. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

h. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiffs' and Class members' PII secure and prevent the loss or misuse of that information;

i. Whether Defendant failed to "implement and maintain reasonable security procedures and practices" for Plaintiffs' and Class members' PII in violation of California Civil Code § 1798.81.5, subdivision (b) and § 5 of the FTC Act;

j. Whether Defendant failed to provide timely notice of the September 2018 Data Breach in violation of California Civil Code § 1798.82;

k. Whether Defendant's conduct violated Cal. Bus. & Prof. Code § 22575, *et seq.;*

l. Whether Defendant owed a duty to Plaintiffs and the Classes to safeguard their

PII and to implement adequate data security measures;

m. Whether Defendant breached that duty;

n. Whether Defendant failed to adhere to its posted privacy policy concerning the care it would take to safeguard Plaintiffs' and Class members' PII in violation of California Business and Professions Code § 22576;

o. Whether Defendant negligently and materially failed to adhere to its posted privacy policy with respect to the extent of its disclosure of users' data, in violation of California Business and Professions Code § 22576;

p. Whether such representations were false with regard to storing and safeguarding Class members' PII; and

q. Whether such representations were material with regard to storing and safeguarding Class members' PII.

CLAIMS ALLEGED ON BEHALF OF ALL CLASSES

First Claim for Relief

Violation of California's Unfair Competition Law ("UCL") – Unlawful Business Practice (Cal. Bus. & Prof. Code § 17200, *et seq*.)

60. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

61. Facebook's terms of service provide that "[f]or any claim, cause of action, or dispute you have against us that arises out of or relates to these Terms or the Facebook Products ("claim")… the laws of the State of California will govern these Terms and any claim."

62. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of the UCL. The conduct alleged herein is a "business practice" within the meaning of the UCL.

63. Facebook represented that it would not disclose Users' PII without consent and/or notice. Facebook further represented that it would utilize sufficient data security protocols and mechanisms to protect Users' PII.

64. Defendant stored the PII of Plaintiffs and members of their respective Classes in Defendant's electronic and consumer information databases. Defendant falsely represented to

Plaintiffs and members of the Classes that the PII databases were secure and that class members' PII would remain private. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied "with federal regulations" and that would have kept Plaintiffs' and the other Class members' PII secure and prevented the loss or misuse of Plaintiffs' and the other class members' PII.

65. Even without these misrepresentations, Plaintiffs and Class members were entitled to assume and did assume, that Defendant would take appropriate measures to keep their PII safe. At no time did Defendant disclose that Plaintiffs' PII was vulnerable to hackers because Defendant's data security measures were inadequate. Such material information was only in the possession of Defendant, which it had a duty to disclose. Defendant violated the UCL by misrepresenting – by affirmative conduct and by omission – the safety of its many systems and services, specifically the security thereof, and its ability to safely store Plaintiff's and Class members' PII. Defendant also violated the UCL by failing to implement reasonable and appropriate security measures or follow industry standards for data security – and failing to comply with its own posted privacy policies. If Defendant had complied with these legal requirements, Plaintiffs and the other Class members would not have suffered the damages described herein.

66. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Cal. Civ. Code § 1798.81.5(b), § 5(a) of the FTC Act, 15 U.S.C. § 45(a), Cal. Bus. & Prof. Code § 22576 (as a result of Facebook failing to comply with its own posted privacy policies).

67. Plaintiffs and the other Class members suffered injury in fact and lost money or property as the result of Defendant's unlawful business practices. Plaintiffs recognize that this Court has ruled that out-of-pocket expenses and the risk of future harm are not sufficient to confer standing under the UCL. However, Plaintiffs' and Class members' PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value (making it clear that information is of tangible value), as a result of the September 2018 Data Breach.

68. As a result of Defendant's unlawful business practices, violations of the UCL,

Plaintiffs and the Class members are entitled to restitution, disgorgement of wrongfully obtained profits, and injunctive relief.

Second Claim for Relief

Violation of California's Unfair Competition Law ("UCL") – Unfair Business Practice (Cal. Bus. & Prof. Code § 17200, *et seq*.)

69. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

70. Facebook's terms of service provide that "[f]or any claim, cause of action, or dispute you have against us that arises out of or relates to these Terms or the Facebook Products ("claim")… the laws of the State of California will govern these Terms and any claim."

71. By reason of the conduct alleged herein, Defendant engaged in unfair "business practices" within the meaning of the UCL.

72. Defendant stored the PII of Plaintiffs and members of their respective Classes in their electronic and consumer information databases. Defendant represented to Plaintiffs and members of the classes that its PII databases were secure and that class members' PII would remain private. Defendant engaged in unfair acts and business practices by representing that it had safeguards which complied with federal regulations to protect PII.

73. Even without these misrepresentations, Plaintiffs and Class members were entitled to, and did, assume that Defendant would take appropriate measures to keep their PII safe. Defendant did not disclose at any time that Plaintiffs' PII was vulnerable to hackers because Defendant's data security measures were inadequate and outdated. Defendant was the only one in possession of that material information, which it had a duty to disclose.

74. Defendant knew or should have known it did not employ reasonable measures to keep Plaintiffs' and the other Class members' PII secure and to prevent the loss or misuse of Plaintiffs' and the other Class members' PII.

75. Defendant violated the UCL by misrepresenting – by affirmative conduct and by omission – the security of its many systems and services and its ability to safely store Plaintiffs' and Class members' PII. Defendant also violated the UCL by failing to

implement and maintain reasonable security procedures and practices appropriate to protect all class members' PII. If Defendant followed the industry standards and legal requirements, Plaintiffs and the Class would not have suffered the damages alleged herein.

76. Defendant also violated its commitment to maintain the confidentiality and security of the PII of Plaintiffs and their respective Classes and failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security.

77. Defendant engaged in unfair business practices under the "balancing test." The harm caused by Defendant's actions and omissions, as described in detail above, greatly outweigh any perceived utility. Indeed, Defendant's failure to follow basic data security protocols and misrepresentations to consumers about Defendant's data security cannot be said to have had any utility at all.

78. Defendant engaged in unfair business practices under the "tethering test." Defendant's actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See, e.g.,* Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(5) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern.") Defendant's acts and omissions, and the injuries caused by them are thus "comparable to or the same as a violation of the law ..." *Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.* (1999) 20 Cal.4th 163, 187.

79. Defendant engaged in unfair business practices under the "FTC test." The harm caused by Defendant's actions and omissions, as described in detail above, is substantial in that it affects approximately 50 million Class members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Class members' PII to

third parties without their consent, diminution in value of their PII, consequential out-of-pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. This harm continues given the fact that Class members' PII remains in Defendant's possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendant's actions and omissions violated, *inter alia*, § 5(a) of the FTC Act, 15 U.S.C. § 45. *See, e.g., F.T.C. v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 613 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015); *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act); *In re BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148, FTC File No. 042-3160 (Sept. 20, 2005) (same); *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168, FTC File No. 052- 3148 (Sept. 5, 2006) (same); *see also United States v. ChoicePoint, Inc.*, Civil Action No. 1:06-cv-0198-JTC (N.D. Ga. Oct. 14, 2009) ("failure to establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers" violates § 5(a) of FTC Act); 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.").

80. Plaintiffs and the other Class members suffered injury in fact and lost money or property as the result of Defendant's unfair business practices. In particular, Plaintiffs and the other Class members have suffered from hacked Facebook accounts and any accounts linked to their Facebook accounts, and other similar harm, all as a result of the September 2018 Data Breach. In addition, their PII was taken and is in the hands of those who will use it for their own advantage or is being sold for value – making it clear that the hacked information is of tangible value. Plaintiffs and Class members have also suffered consequential out-of-pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

81. As a result of Defendant's unfair business practices and violations of the UCL, Plaintiffs and the other Class members are entitled to restitution, disgorgement of wrongfully obtained profits, and injunctive relief.

Third Claim for Relief

Violation of California's Unfair Competition Law ("UCL") – Fraudulent/Deceptive Business Practice (Cal. Bus. & Prof. Code § 17200, *et seq*.)

82. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

83. Facebook engaged in fraudulent and deceptive acts and practices with regard to the services it provided to the Class by representing and advertising that (1) it would maintain adequate data privacy and security practices and procedures to safeguard Class Members' PII from unauthorized disclosure, release, data breaches, and theft and that (2) it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class Members' PII. These representations were likely to deceive members of the public, including Plaintiff and the Class Members, into believing their PII was securely stored – when it was not – and that Facebook was complying with relevant law – when it was not.

84. Facebook engaged in fraudulent and deceptive acts and practices with regard to the services provided to the Class by omitting, suppressing, and concealing the material fact that the privacy and security protections for Class Members' PII was woefully inadequate. At the time that Class members were using Facebook's services, Facebook failed to disclose to Class Members that its data security systems failed to meet legal and industry standards for the protection of their PII. These representations likely deceived members of the public, including Plaintiffs and the Class, into believing that their PII was securely stored – when it was not – and that Facebook was complying with relevant law and industry standards – when it was not.

85. As a direct and proximate result of Facebook's deceptive practices and acts, Plaintiffs and the Class were injured and lost money or property, including but not limited to the loss of their legally protected interest in the confidentiality and privacy of their PII, and additional losses described above.

86. Facebook knew or should have known that its computer systems and data security practices were inadequately safeguarding Class Members' PII and that the risk of a data breach or theft was very high.

87. Facebook's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Class.

88. Class Members seek relief under Cal. Bus. & Prof. Code § 17200, et. seq., including, but not limited to, restitution to Plaintiffs and the Class of money or property that Facebook may have acquired by means of its fraudulent and deceptive business practices, restitutionary disgorgement of all profits accruing to Facebook because of its fraudulent and deceptive business practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

Fourth Claim for Relief

Deceit by Concealment (Cal. Civil Code §§ 1709, 1710)

89. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

90. As alleged above, Defendant knew its data security measures were grossly inadequate by, at the absolute latest, March 2018 when the Cambridge Analytica matter came to light, exposing Facebook's lax and inadequate approach to data security. At that time, Facebook was on notice that its systems were extremely vulnerable to attack – facts that Defendant should have already known given its previous exposures and security problems.

91. In response to all of these facts, Defendant chose to do nothing to protect Plaintiffs and the Class or warn them about the security problems. Instead, Defendant openly represented to Congress and foreign governments that Facebook was dedicated to the highest and most advanced security practices and protocols.

92. Defendant had an obligation to disclose to all class members that their Facebook accounts and PII were an easy target for hackers and Defendant was not implementing measures to protect them.

93. Defendant did not do these things. Instead, Defendant willfully deceived Plaintiffs and the Class by concealing the true facts concerning its poor data security, which Defendant were obligated to, and had a duty to, disclose. Additionally, Facebook made numerous representations following the prior exposures to assure Users that their PII and other data was safe and that Facebook was dedicated to maintaining the security of their data.

94. Had Defendant disclosed the true facts about its poor data security, Plaintiffs and the Class would have taken measures to protect themselves. Plaintiffs and the Class justifiably relied on Defendant to provide accurate and complete information about Defendant's data security, which Defendant failed to do.

95. Alternatively, given the security holes in Defendant's services and Defendant's refusal to take measures to detect those holes, much less fix them, Defendant simply should have shut down their current service. Independent of any representations made by Defendant, Plaintiffs and the Class justifiably relied on Defendant to provide a service with at least minimally adequate security measures and to disclose facts undermining that reliance.

96. Rather than cease offering a clearly unsafe and defective service or disclosing to Plaintiffs and the Class that its services were unsafe and Users' PII was exposed to theft on a grand scale, Defendant continued on, concealing information relating to the inadequacy of its security measures.

97. These actions are "deceit" under Cal. Civil Code § 1710 in that they are the suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact.

98. As a result of this deceit by Defendant, it is liable under Cal. Civil Code § 1709 for "any damage which [Plaintiffs and the Class] thereby suffer[]."

99. As a result of this deceit by Defendant, the PII of Plaintiffs and the Class was compromised, placing them at a greater risk of identity theft or subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiffs and the other Class members also suffered diminution in value of their PII in that it now has become easily available to hackers on the Dark Web. Plaintiffs and the Class have also suffered consequential out-of-

pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

100. Defendant's deceit as alleged herein is fraud under Civil Code § 3294(c)(3) in that it was a deceit or concealment of a material fact known to the Defendant conducted with the intent on the part of Defendant of depriving Plaintiffs and the Class of "legal rights or otherwise causing injury." As a result, Plaintiffs and the Class are entitled to punitive damages against Defendant under Civil Code § 3294(a).

Fifth Claim for Relief
Negligence

101. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

102. Defendant owed a duty to Plaintiffs and the Class to exercise reasonable care in safeguarding and protecting their PII and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, *inter alia*, designing, maintaining, and testing Defendant's security systems to ensure that the PII of Plaintiffs' and the Class was adequately secured and protected, including using encryption technologies. Defendant further had a duty to implement processes that would detect a breach of its security system in a timely manner.

103. Defendant knew that the PII of Plaintiffs and the Class was personal and sensitive information that is valuable to identity thieves and other criminals. Defendant also knew of the serious harms that could happen if the PII of Plaintiffs and the Class was wrongfully disclosed, that disclosure was not fixed, or Plaintiffs and the Class were not told about the disclosure in a timely manner.

104. By entrusting Defendant to safeguard their PII, Plaintiffs and the Class had a special relationship with Defendant. Plaintiffs and the Class signed up for Defendant's services and agreed to provide their PII with the understanding that Defendant would take appropriate measures to protect it, and would inform Plaintiffs and the Class of any breaches or other security concerns that might call for action by Plaintiffs and the Class. But Defendant did not. Defendant

not only knew its data security was inadequate, Defendant also knew it didn't have the tools to detect and document intrusions or exfiltration of PII. Defendant is morally culpable, given its repeated security breaches, wholly inadequate safeguards, and refusal to notify Plaintiffs and the Class of breaches or security vulnerabilities.

105. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite repeated failures and intrusions, and allowing unauthorized access to Plaintiffs' and the other Class members' PII.

106. Defendant's failure to comply with industry and federal regulations further evidences Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class members' PII.

107. Defendant's breaches of these duties were not merely isolated incidents or small mishaps. Rather, the breaches of the duties set forth above resulted from a long-term company-wide refusal by Defendant to acknowledge and correct serious and ongoing data security problems.

108. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and the Class, their PII would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the PII of Plaintiffs and the Class and all resulting damages.

109. The injury and harm suffered by Plaintiffs and the other Class members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other class members' PII. Defendant knew its systems and technologies for processing and securing the PII of Plaintiffs and the Class had numerous security vulnerabilities.

110. As a result of this misconduct by Defendant, the PII of Plaintiffs and the Class were compromised, placing them at a greater risk of identity theft or subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiffs and Class members also suffered diminution in value of their PII in that it is now easily available to

hackers on the Dark Web. Plaintiffs and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

111. Defendant's misconduct as alleged herein is malice or oppression in that it was despicable conduct carried on by Defendant with a willful and conscious disregard of the rights or safety of Plaintiffs and the Class and despicable conduct that has subjected Plaintiffs and the Class to cruel and unjust hardship in conscious disregard of their rights. As a result, Plaintiffs and the Class are entitled to punitive damages against Defendant.

Sixth Claim for Relief

Breach of Implied Contract

112. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

113. Facebook solicited and invited Plaintiffs and Class Members to use its services. Plaintiffs and Class members accepted Facebook's offers and created user accounts requiring the provision of PII with Facebook during the period of the September 2018 Data Breach.

114. When Plaintiffs and Class Members used Facebook services and products, they provided their PII. In so doing, Plaintiffs and Class Members entered into implied contracts with Facebook pursuant to which Facebook agreed to safeguard and protect such information.

115. Each use of a Facebook service or product made by Plaintiffs and Class Members was made pursuant to the mutually agreed-upon implied contract with Facebook under which Facebook agreed to safeguard and protect Plaintiffs and Class Members' PII.

116. Plaintiffs and Class Members would not have provided and entrusted their PII to Facebook in the absence of the implied contract between them and Facebook.

117. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Facebook.

118. Facebook breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect the PII of Plaintiffs and Class.

119. As a direct and proximate result of Facebook's breaches of the implied contracts

between Facebook and Plaintiffs and Class Members, Plaintiffs and Class Members sustained actual losses and damages as described in detail above.

ADDITIONAL CLAIMS ALLEGED ON BEHALF OF THE COLORADO SUB-CLASS ONLY

Seventh Claim for Relief
Violation of Colorado Consumer Protection Act
(Colo. Rev. Stat 6-1-101, *et seq.)*

120. Plaintiffs Johnson and Newborn ("Colorado Plaintiffs") hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

121. Colorado Plaintiffs bring this claim on behalf of the Colorado Sub-Class who are all residents of Colorado.

122. Facebook is a "person" as defined by Colo. Rev. Stat. § 6-1-102(6). Colorado Plaintiffs and Colorado Sub-Class Members are actual or potential consumers of the products and services offered by Facebook.

123. Facebook, operating in Colorado, engaged in deceptive, unfair, and unlawful trade acts or practices in the course of its business, vocation or occupation, in violation of Colo. Rev. Stat. § 6-1-105, including but not limited to the following:

a. Knowingly misrepresenting and fraudulently advertising material facts pertaining to its products and services to the Colorado Sub-Class by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Colorado Sub-Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft, in violation of Colo. Rev. Stat. §§ 6-1-105(e), (g), (i), and (u);

b. Knowingly misrepresenting material facts pertaining to its products and services to the Colorado Sub-Class by representing and advertising that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Colorado Sub-Class Members' Personal Information, in violation of Colo. Rev. Stat. §§ 6-1-105(e), (g), (i), and (u);

c. Knowingly omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Colorado Sub-Class Members' Personal Information (intending to induce others to enter into a transaction), in violation of Colo. Rev. Stat. §§ 6-1-105(e), (g), (i), and (u);

d. Engaging in deceptive, unfair, and unlawful trade acts or practices, in violation of Colo. Rev. Stat. § 6-1-105(3), by failing to maintain the privacy and security of Colorado Sub-Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, including Colo. Rev. Stat. § 6-1-713.5, resulting in the September 2018 Data Breach.

e. Engaging in deceptive, unfair, and unlawful trade acts or practices, in violation of Colo. Rev. Stat. § 6-1-105(3), by failing to disclose the September 2018 Breach to Colorado Sub-Class Members in a timely and accurate manner, contrary to the duties imposed by Colo. Rev. Stat. § 6-1-716(2); and

f. Engaging in deceptive, unfair, and unlawful trade acts or practices, in violation of Colo. Rev. Stat. § 6-1-105(3), by failing to take proper action following the September 2018 Data Breach to enact adequate privacy and security measures and protect Colorado Sub-Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

124. Under Colo. Rev. Stat. § 6-1-713.5, Facebook "maintains, owns, or licenses personal identifying information of an individual residing in [Colorado]," and thus is required to "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations." Facebook failed to maintain reasonable securities procedures and practices appropriate for the nature and size of the business and its operation.

125. Facebook's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Facebook's data security and ability to protect the confidentiality of consumers' Personal Information.

126. Facebook intended to mislead Colorado Plaintiffs and Colorado Sub-Class members and induce them to rely on its misrepresentations and omissions.

127. Had Colorado Plaintiffs and other Colorado Sub-Class Members known that Defendant failed to employ necessary and adequate protection of their personal information, they would not have created a Facebook account or limited the PII they shared with Facebook.

128. Facebook engaged in the above unfair and deceptive acts or practices in the course of its business.

129. Facebook engaged in above unfair and deceptive acts or practices with malice and/or willfulness.

130. As a direct and proximate result of Facebook's unfair and deceptive practices, Colorado Sub-Class Members suffered injuries to legally protected interests, including their legally protected interest in the confidentiality and privacy of their personal information.

131. The above unfair and deceptive practices and acts by Facebook were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Colorado Plaintiffs and Colorado Sub-Class Members that they could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

132. Facebook knew or should have known that its computer systems and data security practices were inadequate to safeguard Colorado Sub-Class Members' Personal Information and that risk of a data breach or theft was high. Facebook's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Colorado Sub-Class.

133. Colorado Plaintiffs and Colorado Sub-Class Members seek relief under Colo. Rev. Stat. §§ 6-1-101, *et seq.*, including, but not limited to, compensatory damages, statutory damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs.

Eighth Claim for Relief
Violation of Colorado Security Breach Notification Act
(Colo. Rev. Stat 6-1-716, *et seq.)*

134. Colorado Plaintiffs hereby repeats, realleges and incorporates by reference each and every allegation contained above as though the same were fully set forth herein.

135. Facebook is a business that owns or licenses computerized data that includes Personal Information as defined by Colo. Rev. Stat. §§ 6-1-716(1) and 6 1-716(2).

136. Colorado Plaintiffs and Colorado Sub-Class PII includes Personal Information as covered by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

137. Under Colo. Rev. Stat. § 6-1-713.5, Facebook "maintains, owns, or licenses personal identifying information of an individual residing in [Colorado]," and thus is required to "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations."

138. Defendant is required to accurately notify Colorado Plaintiffs and Colorado Sub-Class members if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay under Colo. Rev. Stat. § 6-1-716(2).

139. Because Facebook was aware of a breach of its security system, it had an obligation to disclose the September 2018 Data Breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. § 6-1-716(2).

140. By failing to disclose the September 2018 Data Breach in a timely and accurate manner, Facebook violated Colo. Rev. Stat. § 6-1-716(2).

141. As a direct and proximate result of Facebook's violations of Colo. Rev. Stat. § 6-1-716(2), Colorado Plaintiffs and Colorado Sub-Class members suffered damages, as described above.

142. Colorado Plaintiffs and Colorado Sub-Class members seek relief under Colo. Rev. Stat. § 6-1-716(4), including actual damages and equitable relief

ADDITIONAL CLAIMS ALLEGED ON BEHALF OF THE CALIFORNIA SUB-CLASS ONLY

Ninth Claim for Relief
Violation of California Customer Records Act
(California Civil Code § 1798.80, *et seq*.)

143. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

144. Plaintiff King ("California Plaintiff") brings this cause of action on behalf of herself and on behalf of the California Sub-Class who are all California residents.

145. The California Legislature enacted Civil Code § 1798.81.5 "to ensure that personal information about California residents is protected." The statute requires that any business that "owns, licenses, or maintains personal information about a California resident … implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

146. Defendant is a "business" as defined by Civil Code § 1798.80(a).

147. California Plaintiff and California Sub-Class Members are "individual[s]" as defined by Civil Code § 1798.80(d).

148. The personal information taken in the data breach was "personal information" as defined by Civil Code §§ 1798.80(e) and 1798.81.5(d), which includes "information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information."

149. The breach of the personal information of "50 million Facebook users" was a "breach of the security system" of Defendant as defined by Civil Code § 1798.82(g).

150. By failing to implement reasonable security measures appropriate to the nature of the personal information of Facebook Users, Defendant violated Civil Code § 1798.81.5.

151. In addition, by failing to immediately notify all affected Facebook Users that their personal information had been acquired or may have been acquired by unauthorized persons in the data breach, Defendant violated Civil Code § 1798.82.

152. Defendant's failure to immediately notify Facebook Users of the breach caused California Sub-Class Members to suffer damages because they have lost the opportunity to immediately: (i) buy identity protection, monitoring, and recovery services; (ii) flag asset, credit, and tax accounts for fraud, including reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the Internal Revenue Service; (iii) purchase or otherwise obtain credit reports; (iv) monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries, Social Security numbers, home addresses, charges, and/or medical services; (v) place and renew credit fraud alerts on a quarterly basis; (vi) routinely monitor public records, loan data, or criminal records; (vii) contest fraudulent charges and other forms of criminal, financial and medical

identity theft, and repair damage to credit and other financial accounts; and (viii) take other steps to protect themselves and recover from identity theft and fraud.

153. Because they violated Civil Code §§ 1798.81.5 and 1798.82, Defendant "may be enjoined" under Civil Code § 1798.84(e).

154. California Plaintiff requests that the Court enter an injunction requiring Defendant to implement and maintain reasonable security procedures to protect its Users' personal information, including, but not limited to, ordering that Defendants: (a) engage third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis; (b) engage third party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices; (c) audit, test, and train its security personnel regarding any new or modified procedures; (d) purge, delete and destroy, in a secure manner, Facebook Users data not necessary for its business operations; (e) conduct regular database scanning and securing checks consistent with prudent industry practices; (f) periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach consistent with prudent industry practices; (g) receive periodic compliance audits by a third party regarding the security of the computer systems, cloud-based services, and application software Defendant uses to store the personal information of current and former Facebook Users; (h) meaningfully educate its current and former Facebook Users about the threats they face as a result of the loss of their personal information to third parties, as well as the steps they must take to protect themselves; and (i) provide ongoing identity theft protection, monitoring, and recovery services to California Plaintiff and California Sub-Class Members.

155. As a result of Defendant's violation of Cal. Civ. Code § 1798.81.5, California Plaintiff and California Sub-Class Members have incurred and will incur damages, including but not necessarily limited to: (1) the loss of the opportunity to control how their personal information is used; (2) the diminution in the value and/or use of their personal information

entrusted to Defendant for the purpose of deriving services from Defendant and with the understanding that Defendant would safeguard their personal information against theft and not allow access and misuse of their personal information by others; (3) the compromise, publication, and/or theft of their personal information; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (7) unauthorized use of compromised personal information to open new financial and/or health care or medical accounts; (8) tax fraud and/or other unauthorized charges to financial, health care or medical accounts and associated lack of access to funds while proper information is confirmed and corrected; (9) the continued risk to their personal information, which remain in Defendant's possession and are subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the personal information in their possession; and (10) future costs in terms of time, effort and money that will be expended, to prevent, detect, contest, and repair the impact of the personal information compromised as a result of the data breach for the remainder of the lives of the California Sub-Class Members.

156. California Plaintiff seeks all remedies available under Civil Code § 1798.84, including actual and statutory damages, equitable relief, and reasonable attorneys' fees. California Plaintiff also seeks reasonable attorneys' fees and costs under applicable law including California Code of Civil Procedure § 1021.5.

ADDITIONAL CLAIMS ALLEGED ON BEHALF OF THE NEW JERSEY SUB-CLASS ONLY

Tenth Claim for Relief
Violation of New Jersey Customer Security Breach Disclosure Act
(N.J. Stat. Ann. §§ 56:8-163, *et seq*.)

157. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

158. Plaintiff Martin ("New Jersey Plaintiff") brings this cause of action on behalf of herself and on behalf of the New Jersey Sub-Class who are all New Jersey residents.

159. Facebook is a business that compiles or maintains computerized records that include Personal Information on behalf of another business under N.J. Stat. Ann. § 56:8-163(b).

160. New Jersey Plaintiff's and New Jersey Sub-Class members' PII includes Personal Information covered under N.J. Stat. Ann. §§ 56:8-163, *et seq*.

161. Under N.J. Stat. Ann. § 56:8-163(b), "[a]ny business . . . that compiles or maintains computerized records that include Personal Information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers . . . of any breach of security of the computerized records immediately following discovery, if the Personal Information was, or is reasonably believed to have been, accessed by an unauthorized person."

162. Because Facebook discovered a breach of its security system in which Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not secured, Facebook had an obligation to disclose the September 2018 Data Breach in a timely and accurate fashion as mandated under N.J. Stat. Ann. §§ 56:8-163, *et seq*.

163. By failing to disclose the September 2018 Data Breach in a timely and accurate manner, Facebook violated N.J. Stat. Ann. § 56:8-163(b).

164. As a direct and proximate result of Facebook's violations of N.J. Stat. Ann. § 56:8-163(b), New Jersey Plaintiff and New Jersey Sub-Class members suffered the damages described above.

165. New Jersey Plaintiff and New Jersey Sub-Cclass members seek relief under N.J. Stat. Ann. § 56:8-19, including treble damages, attorney's fees and costs, and injunctive relief.

Eleventh Claim for Relief

Violation of New Jersey Consumer Fraud Act

(N.J. Stat. Ann. §§ 56:8-1, *et seq*.)

166. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

167. Plaintiff Martin brings this cause of action on behalf of herself and on behalf of the New Jersey Sub-Class who are all New Jersey residents.

168. Facebook is a "person," as defined by N.J. Stat. Ann. § 56:8-1(d).

169. Facebook sells "merchandise," as defined by N.J. Stat. Ann. § 56:8-1(c) & (e).

170. The New Jersey Consumer Fraud Act, N.J. Stat. §§ 56:8-1, *et seq*., prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

171. Facebook's unconscionable and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect New Jersey Plaintiff and New Jersey Sub-Class members PII, which was a direct and proximate cause of the September 2018 Data Breach;

b. Failing to identify foreseeable security and privacy risks and remediate identified security and privacy risks, which was a direct and proximate cause of the September 2018 Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of New Jersey Plaintiff and New Jersey Sub-Class members' PII, which was a direct and proximate cause of the September 2018 Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of New Jersey Plaintiff and New Jersey Sub-Class members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of New Jersey Plaintiff and New Jersey Sub-Class members' PII;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure New Jersey Plaintiff and New Jersey Sub-Class members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of New Jersey Plaintiff and New Jersey Sub-Class members' PII.

172. Facebook's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Facebook's data security and ability to protect the confidentiality of consumers' PII.

173. Facebook intended to mislead New Jersey Plaintiff and New Jersey Sub-Class members and induce them to rely on its misrepresentations and omissions.

174. Facebook acted intentionally, knowingly, and maliciously to violate New Jersey's Consumer Fraud Act, and recklessly disregarded New Jersey Plaintiff and New Jersey Sub-Class members' rights. Facebook's past data breaches put it on notice that its security and privacy protections were inadequate. Facebook knew its data security measures were grossly inadequate by, at the absolute latest, March 2018 when the Cambridge Analytica matter came to light, exposing Facebook's lax and inadequate approach to data security. At that time Facebook was on notice that its systems were extremely vulnerable to attack – facts that Facebook should have already known given its previous exposures and security problems.

175. As a direct and proximate result of Facebook's unconscionable and deceptive practices, New Jersey Plaintiff and New Jersey Sub-Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

176. New Jersey Plaintiff and New Jersey Sub-Class members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other Class and Sub-Class members, respectfully request that this Court enter an Order:

a. Certifying the United States Class and the Colorado, New Jersey, and California Sub-Classes, and appointing Plaintiffs as Class and Sub-Class Representatives;

b. Finding that Defendant's conduct was negligent, deceptive, unfair, and unlawful as alleged herein;

c. Enjoining Defendant from engaging in further negligent, deceptive, unfair, and unlawful business practices alleged herein;

d. Awarding Plaintiffs and Class and Sub-Class members actual, compensatory, and consequential damages;

e. Awarding Plaintiffs and Class and Sub-Class members statutory damages and penalties, as allowed by law;

f. Awarding Plaintiffs and Class and Sub-Class members restitution and disgorgement;

g. Requiring Defendant to provide appropriate credit monitoring services to Plaintiffs and the other Class and Sub-Class members;

h. Awarding Plaintiffs and Class and Sub-Class members punitive damages;

i. Awarding Plaintiffs and Class and Sub-Class members pre-judgment and post-judgment interest;

j. Awarding Plaintiffs and Class and Sub-Class members reasonable attorneys' fees costs and expenses, and;

k. Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

DATED: October 11, 2018

Respectfully submitted,

/s/ Ivy T. Ngo

Ivy T. Ngo (249860)
Franklin D. Azar & Associates, P.C.
14426 E. Evans Avenue
Aurora, CO 80014
Telephone: 303-757-3300
Facsimile: 720-213-5131
Email: ngoi@fdazar.com